UNIVERSITY OF CALIFORNIA Academic Senate

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING AND COMMUNICATIONS ANNUAL REPORT 2024-2025

TO THE ASSEMBLY OF THE ACADEMIC SENATE:

The University Committee on Academic Computing and Communications (UCACC) is charged in Senate Bylaw 155 to represent the Senate in all matters involving the uses and impact of computing and communications technology and advise the President concerning the acquisition, usage and support of computing and communications technology and related policy issues. UCACC held three meetings via videoconference and one in-person meeting at UCOP in Oakland. In 2024-25, UCACC's primary topics of discussion included campus cybersecurity planning efforts, artificial intelligence, research security, and data storage. Members shared information from their campuses and engaged with administrators at UCOP. This report highlights the committee's discussions and activities during the year.

Cybersecurity

Security Incidents - In December, after a request from UCACC ITS staff presented data about the causes of major cybersecurity incidents at UC. The top 78 incidents from 2024 were categorized by type (e.g., ransomware, human error, phishing, stolen or lost information, etc.). The committee learned that there are millions of attack attempts each year, with even more alerts that are just "noise." The incidents that rise to the "significant" level include breaches involving sensitive data, requiring additional coverage, impact more than 10 individuals, invoke litigation or investigation, involve known criminal activity or a nation-state, or require ransom payment. Later in the year, ITS provided more information about incidents that *were* avoided or *would have been* avoided due to endpoint detection and response (EDR).

President Drake's Cybersecurity Letter and EDR Rollout - Although President Drake's cybersecurity letter was issued in February, as of December 2024, most faculty had not heard of their campus cybersecurity plans or about the mandate from UCOP. Last year, UCACC noted the lack of faculty consultation and foresaw the problems that faculty would have with the EDR requirement for personally owned devices. UCACC encouraged UCOP administrators to communicate broadly regarding the mandate over the course of the year. Local computing committees consulted with CISOs and CIOs, but information was not disseminated thoroughly or consistently within or across the campuses. A "Special" Assembly meeting on February 13th brought attention to the need for better communication at the campus level about cybersecurity efforts. In late spring, pressed to engage further with faculty after resolutions to halt the EDR rollout were circulated on the campuses, the administration hosted a "systemwide informational session on Endpoint Detection and Response (EDR)." UCACC sent CIO Van Williams suggestions for the session, the systemwide FAQ, and moving forward with EDR deployment in consultation with faculty. Nevertheless, many faculty did not feel that their concerns were heard, and a systemwide resolution on the use of Trellix and similar monitoring software was circulated and approved by the Assembly of the Academic Senate on June 12th.

Throughout the year, UCACC pressed for a systemwide user-level FAQ about EDR, with clear information describing what data is collected, who can view it, and how long it is retained. UCACC suggested that examples or use cases would help clarify for faculty how EDR software would be used.

UCACC reviewed a working draft standards document for MFA and EDR implementation. These are not published documents but are used by IT units on the campuses as guidance.

Training - UCACC was informed that UC plans to replace its current cybersecurity training in the next year or two and anticipates moving away from compliance-based videos to just-in-time or error-based user-targeted efforts. To counter resistance, UCACC suggested that better communication would be helpful for faculty to clearly understand that training and security requirements protect them and their work. There continues to be interest in metrics about the efficacy of EDR, training videos, and other mandated controls.

Artificial Intelligence

AI Council – UCACC continued to learn about the UC Council on Artificial Intelligence (AI), a systemwide group appointed by the president and co-chaired by UCSF Professor Alex Bui and UCOP Chief Compliance Officer Alex Bustamante. UCACC member Duygu Tosun-Turgut (UCSF) served as the Academic Senate's representative to the Council and provided regular updates. In October, UCACC was joined by Systemwide Deputy Audit Officer Matt Hicks for an update on the work of the Risk Management Subcommittee of the UC AI Council, including a new risk assessment guide written for administrators to help evaluate the risks associated with use of AI in administrative settings.

Publisher Agreements – In February, Associate Vice Provost and California Digital Library (CDL) Executive Director Günter Waibel joined UCACC's meeting to introduce an issue concerning publisher license agreements that restrict the ability of researchers to perform AI text and data mining. A major publisher has started to require permission for any text and data mining, which UC considers fair use. CDL, which maintains all digital publishing licenses for the UC system, is concerned about the chilling effect caused by barriers to open research. UCACC members were asked to report back if this was impacting colleagues.

Academic Uses of AI – UCACC members Lisa Yeo (UCM) and Igor Mezic (UCSB) participated in the systemwide Senate's Faculty AI Workgroup and provided updates on that group's discussions. Committee members want to ensure that faculty have a voice in decisions about the acquisition and use of AI tools. Ensuring consideration of high standards of scholarship in the face of increasing AI adoption is an ongoing discussion.

Additional Business

Campus IT Governance Structure – UCACC discussed local IT governance and updated the Campus IT Governance Structures chart (shared via Google docs) that tracks faculty involvement in campus IT governance at each campus.

Research Data Backup System – The Research Data Backup System (RDBS) Steering Committee that was active last year has paused its work after evaluating the results of an RFP for a common UC data backup solution. Campuses can now use a vetted solution for their storage backup needs, although there is no systemwide funding.

Data Storage Concerns – UCACC talked about data storage constraints and shared practices and proposals for equitably offering more to those faculty who need it.

UC's IT Accessibility Policy – In October, UCACC heard about proposed revisions to UC's IT Accessibility Policy that are required by new digital access regulations enacted under the ADA. Conforming with new regulations will be expensive and challenging. ITS has requested funding for an additional accessibility FTE for each location and UC is forming a Center of Excellence to provide systemwide support.

Systemwide IT Procurement – Senior Manager for IT Strategic Sourcing Roshni Pratap joined UCACC's October meeting to talk about UC's license agreements with OpenAI and Adobe.

Central Cyber Risk Unit – UCACC learned more about the new central cyber risk unit formed within ITS at UCOP that will try to streamline risk assessment activities, including vendor risk assessments (VRA). The plan is to have a central repository and systemwide methodology. Many will be pleased to hear that VRA exemptions will be considered for low-risk suppliers.

UCPath Security Controls Upgrade – UCOP Chief Information Security Officer April Sather informed UCACC about increased security requirements for UCPath that are needed due to increasingly prevalent instances of direct deposit fraud.

Systemwide and Campus Updates*:* UCACC devoted part of each regular meeting to discussing systemwide issues as reported by Academic Senate leadership and reports from campus representatives on individual campus activities and concerns.

REPRESENTATION

UCACC Chair Jenson Wong served as a faculty representative to the CIO Council and as an *ex officio* member of the University Committee on Library and Scholarly Communications (UCOLASC). Chair Wong also served as Senate representative to the Cyber-Risk Governance Committee (CRGC). Duygu Tosun-Turgot (UCSF) served as the Academic Senate liaison to the UC Artificial Intelligence (AI) Council. Lisa Yeo (UCM) and Igor Mezić (UCSB) served on the Faculty AI Workgroup.

ACKNOWLEDGEMENTS

UCACC is grateful for the contributions made by the consultants and guests who attended meetings in 2024-25, including:

- Matthew Hicks, Systemwide Deputy Audit Officer, UC Office of Ethics, Compliance and Audit Services
- Roshni Pratap, Senior Manager for IT Strategic Sourcing, UC Procurement Services
- Monte Ratzlaff, UC Cyber-Risk Program Director and Interim UC Chief Information Security Officer
- April Sather, UCOP Chief Information Security Officer
- Günter Waibel, Associate Vice Provost & Executive Director, California Digital Library
- Van Williams, Chief Information Officer and Vice President for Information Technology Services

RESPECTFULLY SUBMITTED,

Jenson Wong, Chair (UC San Francisco)
George Porter, Vice Chair (UC San Diego)
John Kubiatowicz (UC Berkeley)
Jeremy Mason (UC Davis)

Paul Gershon (UC Irvine)
Irene Chen (UCLA)
Lisa Yeo (UC Merced)
Ilya Brookwell (UC Riverside)
Barry Grant (UC San Diego)
Duygu Tosun-Turgut (UC San Francisco)
Igor Mezić (UC Santa Barbara)
Jerome Fiechter (UC Santa Cruz)
Steven Cheung, Academic Council Chair *(Ex Officio)*
Ahmet Palazoglu, Academic Council Vice Chair *(Ex Officio)*
Partho Ghosh, CCGA Vice Chair *(Ex Officio)*
Kathrin Plath, UCOLASC Vice Chair *(Ex Officio)*
Joanne Miller, Committee Analyst